Whitepaper

Security advantage for Webex

webex by CISCO

Contents

A majority of Fortune 100 companies use Cisco for their security needs.

Based on Cisco's decades-long rich history of security, Webex gives you data security, compliance visibility, and control over your meetings. Inside your own organization, or even when collaborating across company lines, you get a hardened collaboration platform that helps keep your data secure.

Webex provides you with a single platform for calling, meeting, messaging, whiteboarding, video devices, and Unified Contact Center. We build all products in accordance with the Cisco Secure Development Lifecycle (SDL), which includes privacy impact assessments, proactive penetration testing, and threat modelling. Cisco's Security and Trust organization oversees security and privacy for Webex, and publicly discloses security vulnerabilities.

Privacy, security, and transparency

Our three security principles:

- Webex is committed to respecting the **privacy** of your data.
- Webex is **secure** by default.
- Webex has **security cyber governance** and is **transparent** when there are security issues.

Data privacy and security processes

Table 1 outlines the privacy and security features built into the Webex portfolio of products.

Table 1. Webex privacy and security policies, processes, capabilities, and commitments

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
Strict privacy policy	• Webex does not share, rent, or sell customer information with any third parties.
Security and privacy governance	• An independent security and trust organization exists and is separate from the product engineering organization to avoid conflicts of interest. • A companywide data protection and privacy program assures customers their data is private. • Cisco Trust Center. • Cisco Secure Development Lifecycle (SDL)
Transparent reporting of security issue or fixes	• Dedicated 24x7 global Product Security Incident Response Team (PSIRT) to manage receipt and public disclosure of security vulnerabilities. • Cisco Emergency Response, including CSIRT for comprehensive investigation and prevention of threats. • Letters of attestation on outcomes of penetration testing available under NDA.
Customer data residency choices	• Customers can select the region to store Webex data and user identities. • Encryption keys are generated and managed in your home region. • Ability to pin media to a specific region for Meetings exists.

Table 1. Webex privacy and security policies, processes, capabilities, and commitments

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
Cisco Trust Center and data privacy programs	• Cisco hosts a Trust Center to ensure privacy and transparency needs of our customers are addressed. • Cisco's Trust Center is our platform for sharing our commitment to security, trust, data protection, and privacy. • Cisco's Trust Center hosts has over 56 privacy data sheets and data maps. • Cisco's Trust Portal is an on-demand delivery platform for public and confidential security assurance documentation. Customers can download white papers, privacy data sheets, and more. • Privacy data sheets are reviewed and kept up to date by Cisco legal and security teams. • Cisco has our own data privacy office and also has three regional data privacy officers, who keep up to date with regional privacy requirements to ensure products align with requirements in the Americas, EMEAR, and APAC.
Cisco Secure Development Lifecycle (SDL)	• Product security baseline—more than 200 specific security requirements. • Threat modelling –identify, assess, and mitigate risk for 1000+ features per quarter. • Privacy and Data Impact Assessment of all new features. • Mandatory security training for product and engineering—over 35,000 employees have been certified. • Employee Code of Conduct. • Annual employee training on data privacy, data categorization, and data handling.
Cisco Cloud Access Provider Review (CASPR) of third parties	• Due diligence of third-party cloud vendor's security and assessment of its privacy practices. • Master Data Protection Agreements (MDPAs) exist between Cisco and our affiliates to mitigate risk associated with the supply of products and/or services by Cisco to customers. • Vendor Risk Assessment.
Secure DevOps	• Corporate network and multifactor authentication access for the corporate production environment. • Role-based and least privilege access. • Quarterly user access reviews. • Regular vulnerability scans. • Continuous penetration testing by external and internal teams—cloud and hybrid services. • Continuous production asset inventory. • Asset disposal inventory. • Logically separated production and non-production environments.

Table 1. Webex privacy and security policies, processes, capabilities, and commitments

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
Security and privacy certifications	• ISO 27001 / 27017 / 27018. • SOC 2 Type II and SOC 3. • Cloud Computing Compliance Controls Catalog (C5). • HITRUST (Teams). • FedRAMP Moderate (Meetings, Teams, UCMC-G). • Cisco's Quality Management System ISO 9001.
Regulatory compliance	• HIPAA • FERPA • COPPA • CIPA • EU GDPR • Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). • Personal Health Information Protection Act (PHIPA).
Cross-border transfers	• Binding corporate rules. • EU-US privacy shield. • Swiss-U.S. privacy shield. • APEC cross-border privacy rules. • APEC privacy recognition for processors. • EU standard contractual clauses.

Customers entrust Webex with their mission-critical collaboration, meetings, messages, calling, and data.

Protecting the data ensures compliance with global privacy laws and regulations and reduces risk of exposure to competitors, proprietary information becoming public, loss of trust, recovery costs, fines, unwanted press, and a bad reputation.

Webex provides a hardened collaboration platform that helps keep customers' data secure. Webex does this by making privacy and security the top priority in the design, development, deployment, and maintenance of our networks, platforms, and applications. Webex employs multiple technologies, procedures, and teams to ensure the collaboration platform meets privacy and security requirements.

- Cisco has a mature Secure Development Lifecycle, which is a repeatable and measurable process that includes: security requirements, threat modelling, secure design and coding, static analysis, vulnerability testing, privacy impact assessments, and third-party security assessments.
- Webex has a security assessment program to assess and remediate vulnerabilities in the environment on an ongoing basis.
- Webex manages access to systems for administration and support based on "need to know," separation of duties, role-based access, and multi-factor authentication.
- Webex monitors networks and systems to detect outages, service latency, security incidents, and other unusual and unauthorized activities and events. Personnel are always on call to ensure that alarms are addressed.
- The Cisco Product Security Incident Response Team responds to product security incidents. The Cisco Computer Security (and Data) Incident Response Team provides proactive threat analysis, incident detection, and internally coordinated security incident response.
- Independent external and internal audits and risk assessments are performed on an ongoing basis. Webex is committed to resolving areas of improvement that may be identified.
- Cisco's commitment to customers is open and transparent. Cisco clearly communicates with customers about technical or other issues that could potentially expose their organizations to risk. Penetration results are available to customers under Non-Disclosure Agreements (NDA).
- Cisco has a privacy program based on privacy by design in order to protect our customers' Personally Identifiable Information (PII). The program includes a Privacy Impact Assessment (PIA), incident response, notice to customers, and management of subject requests.
- A privacy and security awareness education and training program is required for all staff while onboarding and again annually.
- The Cisco collaboration chief security officer and security team are part of Cisco's Security and Trust Organization (S&TO). The S&TO is independent of the Webex organization and enforces privacy and security policies. The security team ensures compliance with processes, performs assessments, and provides guidance to engineering and operations teams.

References

- Trust Center
- Trustworthy Solutions
- CSDL
- Data Protection Program
- Privacy at Cisco

Securing your users and identity

Table 2 outlines capabilities available within the Webex portfolio of products to secure users and identities.

Table 2. Securing users and identity

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
Automated enterprise-grade user provisioning and lifecycle management in Control Hub	• Active Directory synchronization: This one-way sync ensures users are not only provisioned when onboarded to the enterprise (reducing your total cost of ownership), but more importantly, it ensures users are deprovisioned and tokens are revoked when the enterprise decides they should be deprovisioned. • Identity proofing: Admins verify their domains to ensure the users they provision are who they say they are so when you join a meeting you can trust who you are collaborating with. • System for Cross-domain Identity Management (SCIM) provisioning: Onboard users through Okta and Azure AD integrations using SCIM, the industry standard. Cisco, taking advantage of our relationships in the industry, is continuously adding leading identity providers to the list of products that we support. Because Cisco uses standards instead of proprietary protocols, we can add new IdPs faster. • People API on Developer.webex.com and CSV are also supported.
Multi-Factor Authentication (MFA)	• Webex Identity Service provides MFA multifactor authentication to provide secure remote collaboration. One option is to use Cisco Duo with your Webex deployment. This can be deployed as an option as a second factor with your IdP (PingIdentity, Forgerock, Microsoft, or Okta).
Oauth2.0-based standardized authorization (not software development kits)	• All integrations use a client ID and client secret, and in the authorization grant flow, show the users what scopes are shared with the third-party integration.
Identity obfuscation across services	• User identity information is stored in the customer's selected data residency region at the time of provisioning. Only obfuscated IDs are used by services instead of user email addresses.
Support for SSO with customer choice of identity provider (IdP)	• Supported on-premises IdPs – Ping Identity, ADFS, ForgeRock, Shibboleth, OracleAM, IBM Secure Access Manager, F5 BigIP. • Supported IDaaS partners – Microsoft Azure AD, Okta, PingOne, LastPass, Simplified, OneLogin, OnePassword.

Table 2. Securing users and identity

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
Blocking use of a personal account login to Webex	Reduce data loss concerns so users can only use their company email Webex on the corporate network.
Risk-based authentication to stop the risk at the point of access or adapt to the changing user authentication environment	Webex has worked with the leading IdP providers and support zero-trust solutions, including Cisco Duo, Okta, Microsoft AzureAD, ForgeRock, and Ping Identity to integrate with their risk-based authentication modules. Using these solutions in concert with Security, customers can manage access. Use 30 different values, including IP address, location, device fingerprinting, login history, and geolocation with machine learning and AI to provide the right authentication challenge for right situation.

User provisioning and lifecycle management

User lifecycle management

Cisco Common Identity provides the secure identity management, directory services, and authentication and authorization for users, groups, bots, and devices. This ensures that customers can trust who they are collaborating with for critical business and personal activities. This trust is maintained throughout the lifecycle, from proofing the users before they are created, updated, and deleted.

Active Directory synchronization

This one-way sync ensures users are not only provisioned when onboarded to the enterprise (reducing your total cost of ownership), but more importantly, ensures that users are deprovisioned and tokens are revoked when the enterprise decides they should be deprovisioned.

Identity proofing

Admins verify their domains to ensure the users they provision are who they say they are so when you join a meeting you can trust who you are collaborating with. This proofing mechanism ensures the administrator has the rights to the domain they verify so users can be created without having to receive an email or go through another proofing service to verify their identity.

SCIM user provisioning

Customers can onboard users through Okta and Azure AD integrations using SCIM, the industry standard. Taking advantage of our relationships in the industry, Cisco continuously adds leading identity providers to the list of products that we support. Because Cisco uses standards instead of proprietary protocols, we can add new IdPs faster.

Additional user provisioning

The Control Hub allows partners, developers, and customers to provision users via APIs and CSV support.

Authentication and authorization

Cisco uses standards-based methods to provide a secure method of authentication and authorization for a user, whether they are a small business or a f ederal government agency requiring the highest level of security. If the organization uses a username and password, Webex provides a minimum-level password complexity that meets the U.S. National Institute of Standards and Technology (NIST) guidelines. If a customer requires a need to increase the entropy of passwords, the customer can change the password complexity by changing factors (e.g., number of characters required, special characters, uppercase, and numbers).

Security Assertion Markup Language (SAML) 2.0 Single-Sign-On: Cisco uses SAML 2.0 to federate authentication to the leading identity providers in the market. These include:

- Supported on-premises IdPs, such as Ping Identity, ADFS, ForgeRock, Shibboleth, OracleAM, IBM Secure Access Manager, F5 BigIP
- Supported IDaaS partners, including Microsoft Azure AD, Okta, PingOne, LastPass, Simplified, OneLogin, OnePassword

This allows enterprises to redirect users from Webex to their IdP and allow them to use the password and authentication flows users use for thousands of different applications provided by their employer. This also allows them to use any second factor for authentication as part of their flow.

Multi-factor authentication
Most people today use less than five passwords across their different Internet sites, allowing attackers the ability to replay passwords from compromised sites in other accounts until they find a site where that password has been reused. Cisco Duo is the leading multifactor solution in the market. When paired with Control Hub and a leading identity provider for lifecycle management, Duo offers a zero-trust collaboration environment. Cisco Duo provides more than just MFA; it can also identify risky devices, enforce contextual access policies, and report on device health using an agentless approach or by integrating with your device management tools.

Risk-based authentication
Webex has worked with leading IdP providers and zero-trust solutions like Cisco Duo, Okta, Microsoft AzureAD, ForgeRock, and Ping Identity to integrate with these vendors' risk-based authentication modules. Using these solutions in concert with Security, a customer can manage access. Use 30 different values, including IP address, location, device fingerprinting, login history, and geolocation with machine learning and AI to provide the right authentication challenge for right situation. Paired with SCIM-based provisioning, these risk-based engines can also inactivate users, so they lose access immediately.

Blocking use of a personal account login to Webex
Enterprises may want to ensure that all users are using only their corporate accounts to access Webex. Cisco has worked with leading network proxies like Web Security Appliance (WSA) to add a rule that specifies which domains are allowed to authenticate to Webex. For example, if acme.com only wants users from acme.com to authenticate, the company can specify acme.com in the rule and Webex will inspect the authentication header and deny authentication from all users that do not have acme.com domains. Learn more about how to configure this option on the CiscoSupport site.

Securing your apps and devices

Table 3 outlines Webex capabilities to secure apps and devices.

Table 3. Securing apps and devices

CAPABILITIES	WEBEX
MAM app wrapping process	Supported in Webex
MDM verification	Supported in Webex
AppConfig support	Supported in Webex
Microsoft Intune SDK support	Supported in Webex
Facial recognition and fingerprint recognition for mobile login	Supported in Webex Meetings
Remote wipe: Webex native security controls	Supported in Webex
Pin-lock requirement: Webex native security control	Supported in Webex
File share controls by device type: native security control	Supported in Webex
File share controls based on IP ranges	Supported in Webex
File share controls based on Active Directory groups	Supported in Webex
Full encryption of local cache on clients	Supported for Webex desktop and mobile clients
Custom idle time out for Web App and Control Hub	Supported for Webex browser-based clients and Control Hub

MAM app wrapping

A customer who would like to support a BYOD environment usually requires containerization of enterprise applications. With the option to allow a customer to perform app wrapping through their choice of MAM providers to Webex mobile apps, a customer can more safely onboard their users to Webex in a manner that meets their enterprise compliance requirements.

MDM verification

All Webex mobile apps have been verified with Multiple Device Management (MDM) providers for controls that can be applied in the app, such as preventing copying/pasting or remotely deleting the application and many others.

AppConfig support

IT administrators can control user access to app functions such as sign-in methods, meeting sources, video access, and others by using an MDM AppConfig service to configure the Webex Meetings and Webex Messaging applications on managed mobile devices.

Microsoft Intune SDK support

Webex mobile applications support Microsoft Intune integration with a Software Development Kit (SDK). With this SDK, IT administrators can control user access to application functions and configuration policies for Webex Meetings and Messaging, in order to control and secure corporate data.

Webex native security controls

Webex App can be managed and controlled through many natively built controls, which can be used by customers who have an environment of BYOD and do not use MAM. Some examples include:

- **Remote wipe and reset**: When a device is lost or a user has left the company, an administrator can remotely wipe the content on the device, and therefore, secure the intellectual property of the company.
- **Requiring PIN lock**: A customer who has a BYOD environment can ensure their users will have pin lock set on their personally managed devices in order to use the Webex mobile app.
- **File share controls**: A customer who has a locked-down environment can ensure their users can upload and download files only from the preferred client type (desktop instead of mobile, for example).
- **Disabling message preview**: A customer can ensure that message previews for mobile notifications are always disabled so that nearby users cannot peek into the messages being exchanged. Or if the device is locked and left behind inadvertently, other users do not continue to see previews of messages being sent by looking at the device's locked screen.
- **Encrypted local cache**: As an industry-first standard, Webex, which supports the messaging workload, stores content in a local database and is always fully encrypted.
- **Custom idle time out for browser interfaces**: A Webex administrator using Control Hub, or a user using the browser-based Teams interface, do not have to worry about leaving their laptop unattended. A capability to set custom time out in Control Hub allows an administrator to reduce the security risk of such events by terminating idle sessions after a period of time outs (anywhere between 10 minutes to 60 minutes). The Control Hub also has a default idle timeout of 20 minutes. These timeouts can be customized further for in network and out of network. If a user is logging into the system in the security of VPN, the company network idle timeout period can be longer (or never turned on), and durations can be made shorter if they are on a public network.

Securing your content by default

Table 4 outlines Webex capabilities to secure content by default.

Table 4. Securing content

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
End-to-end encryption for Webex Meetings	• This optional control enables a meeting host to allow encryption when using the Webex Meetings. • Highly scalable. • The meeting encryption key is generated by the meeting host and securely distributed to meeting participants. The cloud does not have access to meeting encryption keys.
End-to-end encryption in Webex	• User-generated content (messages and files) that are shared in Webex spaces are encrypted end to end by the Webex App before being sent to the cloud over TLS, with a few exceptions. This user-generated content is stored in its encrypted form in the cloud. • End-to-end encryption keys are created for each Webex space using a Webex Key Management Service (KMS). • Customers can choose to use the cloud-based KMS or deploy the KMS on their premises (as part of our Hybrid Data Security [HDS] service), which allows customers to hold keys.
In-house transcription of recordings	• All recordings and transcriptions are AES256-encrypted and stored at rest in the cloud. • Recordings are encrypted with an HSM derived key. • HSM is hosted and operated by a separate Cisco security team. The Webex Meetings team does not have access to the keys. • Customer data is not used for transcription service training.
Secure your content sharing	• Restrict the viewing of recordings to signed-in users only. • Prevent the download of recordings. • Enforce passwords for all network-based recordings. • Enable/disable content sharing with external integrations. • Restrict application sharing (Meetings). • Granular controls are available to prevent desktop, application, whiteboard, and file sharing (meetings).

Flexible admin control for security

Tables 5 outlines security controls for Webex admins.

Table 5. Admin security control functions

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX
Prevent unauthorized attendees from joining meetings	• Use unique password-protected link for users with an invitation only (default). • Automatically lock meeting rooms to restrict entry (default). • Automatically put external or unauthenticated attendees in a waiting room (default). • Enforce passwords or sign-on for phones and video devices.
Prevent disruptions during meeting	• Prevent the ability to join a meeting before the host. • Manually lock your room. • Prevent share grabbing. • Configure your room to automatically lock after a specified duration. • Make participants who join a Personal Room that is locked to be placed in the lobby until admitted by the host.
Limit meetings to internal users only	• Enforce SSO for joining or Personal Meeting Room entry. • Require attendee roles.
Prevent forwarding of invitations	• Enforce that only invited users can join meetings.
Empower a host to securely manage a Personal Room meeting	• Visual difference in internal/external users in roster. • Entry and exit tones. • Lock the room. • Enable an email notification to be sent to you in the event someone enters your Personal Room lobby while you are away. • Enable/disable available functions such as chat, video, voice options. • Expel, lock, mute, etc.
Manage file sharing control	• The admin can choose to selectively enable or disable file sharing (Meetings and Messaging). • The admin can limit file sharing based on client type (Webex Messaging).
Manage external integrations (Meetings & Teams)	Supported in Webex
Manage bots	Supported in Webex

Manage external integration

A customer can allow or deny their users to integrate Google accounts, Microsoft Office 365 accounts, Facebook accounts, and other third-party applications with their Webex account. In addition, customers can also ensure that only those third-party apps for Webex (developed using APIs from developer.webex.com) that meet their security and data handling standards can be enabled for their users. Customers can choose to allow or deny access to these third-party apps for everyone in the organization or to specific users.

Manage bots

A customer can manage bots for Webex spaces, such as external integrations management, to control the outflow of information and reduce risk. Administrators can set global policies to allow or deny bots for their organization. In case of "global deny," individual bots can be allowed and therefore made available in group and direct spaces for organizational employees to communicate with.

Block external communication

The Block External Communications function allows admins to control cross-organization collaboration in the following ways:

- All users in your organization are restricted from communicating with anyone in external organizations in Webex
- Users within the organization cannot add users outside the approved domains or join spaces created by non-approved domains in Webex
- Use the attendee role and the "Require login before site access" control to block participants who are external to your Meetings site (Figure 1)

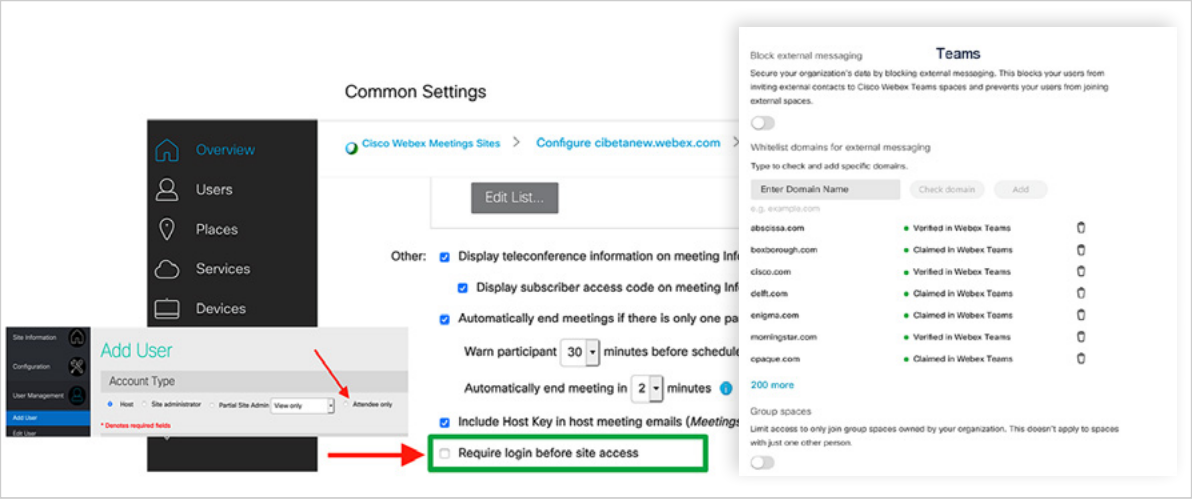

Figure 1. Block external communications features

Built-in compliance tools eliminate the need for third-party solutions

Tables 6 covers compliance tools customers can use to remove the need for third-party solutions.

Table 6. Available compliance tools

CAPABILITIES	WEBEX
Flexible retention control	Use a flexible and customizable retention policy: • From 7 days up to 12 months of retention of recordings with unlimited storage (Webex Meetings). • From 30 days up to indefinite retention for messages and files (Webex Messaging).
Legal hold	• Native support for Webex Messaging for user-generated content (messages and files).
eDiscovery	• Native support for Webex Messaging for user-generated content (messages and files).

Control Hub's built-in compliance tools provide a single solution to help organizations ensure compliance, reduce risk and cost, and eliminate the need for a third-party compliance solution. You can collect, preserve, review, and export all your electronic communications data on demand with a flexible retention policy, legal hold, and eDiscovery features purpose-built for regulated organizations.

Flexible retention

Organizations can manage risks and align with corporate retention policies by setting a custom retention period in Control Hub. An administrator can define an organization-wide retention policy in Webex or a site-level data retention policy for Webex Meetings, so that all relevant contents are permanently deleted at the configured retention timeframe. This reduces the risk of confidential information being accessible for a long time and also helps with alignment to retention policies across email and other applications.

Legal hold

In order to help you with compliance requirements to support legal investigations, Control Hub's legal hold tool makes it easy for your organization to preserve all forms of user-generated content related to litigation or investigation, all without impacting the end-user experience.

Compliance officers can create a legal matter and put custodians (users) on legal hold, view and download matters, and release matters (Figure 2). Data on legal hold is not subject to deletion based on the organization's retention period. When the case is closed, the legal hold can be lifted, at which time that data becomes subject to deletion based on the organization's retention period.

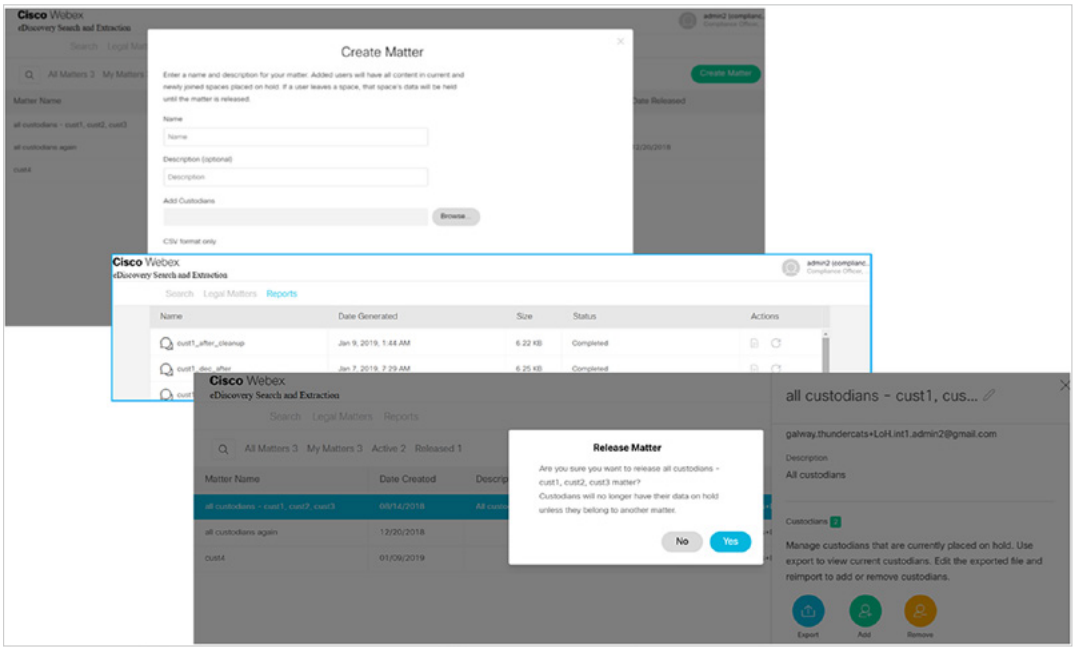

Figure 2. Create, view, and release matters

eDiscovery

Control Hub's built-in eDiscovery search tool provides the ability to search and extract content generated by specific custodians (users) across a time range of interest. As a compliance officer, you can use eDiscovery to search through any conversation in the Webex App (Figure 3). You can look for a specific person in your company, find content they've shared, or search through a specific space and then generate a report of your findings. This helps compliance officers and legal counsel gather data for legal, HR and regulatory investigations in a self-serve manner.

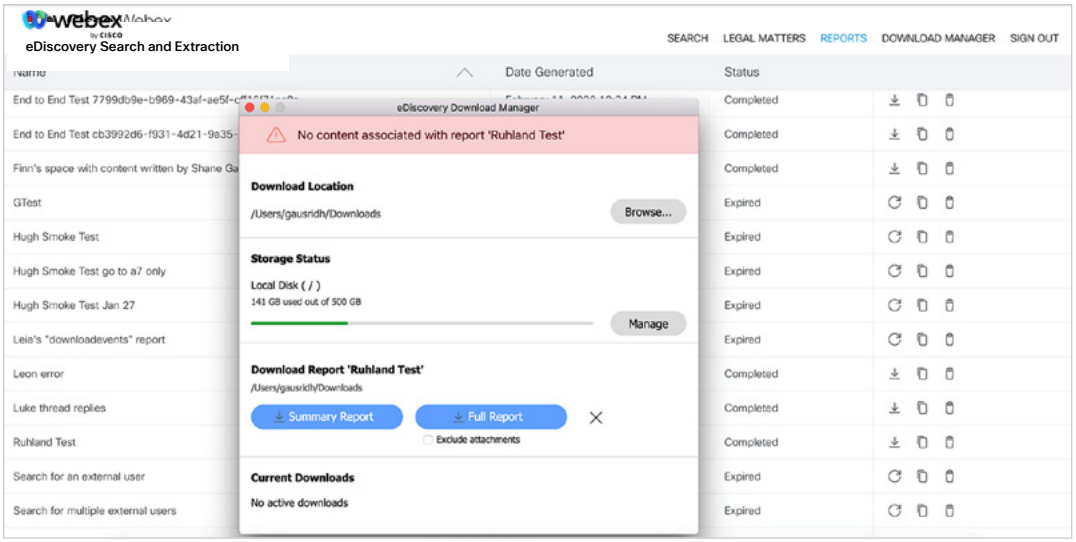

Figure 3. Search data within Webex

Data loss protection

Tables 7 details data loss protection capabilities built into Webex products.

Table 7. Available data loss protection capabilities

CAPABILITIES	WEBEX
Protect sensitive data leakage	• Integrated data loss protection with Cisco Cloudlock® and third parties for Webex. • Detection and remediation policies purpose-built and tuned for Webex (space memberships, message, and file-based violations). • Out-of-the-box policies for several regulated industry verticals (finance, healthcare, etc.) to accelerate deployment time.
DLP and archival partner ecosystem	• Extensive partner ecosystem with over 10 industry-leading archival and data loss protection/ Cloud Access Security Broker (CASB) vendors for messaging and meetings. • Prebuilt and tested integrations result in faster time to market and reduce custom development work. • A large partner ecosystem gives customers the option to use existing data loss protection products from their partner vendors.
Cross-organizational policies	• Block all external communication. • Allow external communication with specific domains.
Space classifications	• Allow admins to enforce end-user classification of spaces created in Webex. • Prevents inadvertent loss of confidential and sensitive information.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) tools help prevent loss or unauthorized access of sensitive data and are an integral part of securing collaboration applications. ADLP engine scans content generated by users and identifies and provides visibility into policy violations. It is imperative that DLP policy engines support a rich set of predefined policies across industry verticals such as finance (routing number, bank account number), healthcare (PII, drug name), education (student loan information, FERPA), and many more that result in the most common data compromise scenarios.

In addition, enterprises need the ability to create custom policies tailored to their business needs and risk posture. If a violation is identified, the DLP engine must enforce remediation action, such as sending alerts (to end users and admins), removing users from messaging in spaces, and deleting offending user-generated content (chat messages, files, etc.). These remediating actions ensure that users don't accidentally or maliciously share sensitive data that could put an organization at risk.

The risk and negative impact of data loss increases significantly when communication boundaries expand outside an organization.

Cloud applications and collaboration platforms should provide access to user-generated data and critical events via public APIs, or by other means to DLP engines. A good ecosystem of DLP vendors is also important to ensure that customers have a choice and can continue to leverage their investment in an existing DLP / CASB vendor. The detection algorithm used by the DLP engine must be tuned to best fit the collaboration use cases, content type, and context. Collaboration platforms often become a black box with little to no visibility when users generate content in another organization's space (or tenant). This is a high-risk scenario with potential data exfiltration that can go undetected.

Webex offers public REST APIs (referred to as events API) that partners can call to retrieve data generated by all users within their organization. The public interfaces allow any partner to integrate with the Webex to retrieve events of interest and enforce policies in a timely manner. The pre-built integration offered via the Webex Extended Security Pack reduces time to market and helps prevents loss of critical data and intellectual property.

Figures 4 and 5 provide screenshots of ways to use the DLP policies functions within Webex products.

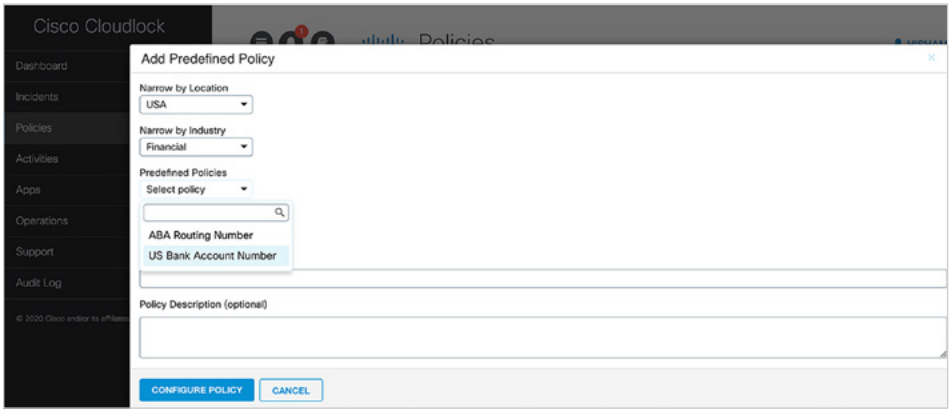

Figure 4. Configuring a predefined U.S. financial industry policy

Figure 5. Incident dashboard highlighting violations

Space classifications

The space classifications feature allows organizational administrators to define classification labels based on data governance policies and enforce all users to classify spaces they create, such as public, confidential, highly confidential, and secret. The feature provides admins the ability to edit and disable existing classifications and also add new classifications, allowing organizations to mature their classification taxonomy and standards over time.

An intuitive client visual design alerts users about the classification level of spaces, making them aware of the space classification context and helping them remain compliant when handling sensitive data. A prominent classification badge in the message compose area within each classified space alerts users about the confidential nature of the space and also helps minimizes inadvertent loss of data.

DLP partners can leverage the compliance APIs to consume classification events and apply a rich set of content and context-based policies to eliminate the compromise of intellectual property and data. This feature can help an organization's users adhere to enterprise-wide data governance policies related to sharing of confidential information in an automated manner by applying rules (e.g., no external participant in a space where confidential data is shared) that govern the sharing of data using the APIs provided.

Note: Policies have to be applied in an external DLP engine and are not supported natively; the Webex provides the required APIs only.

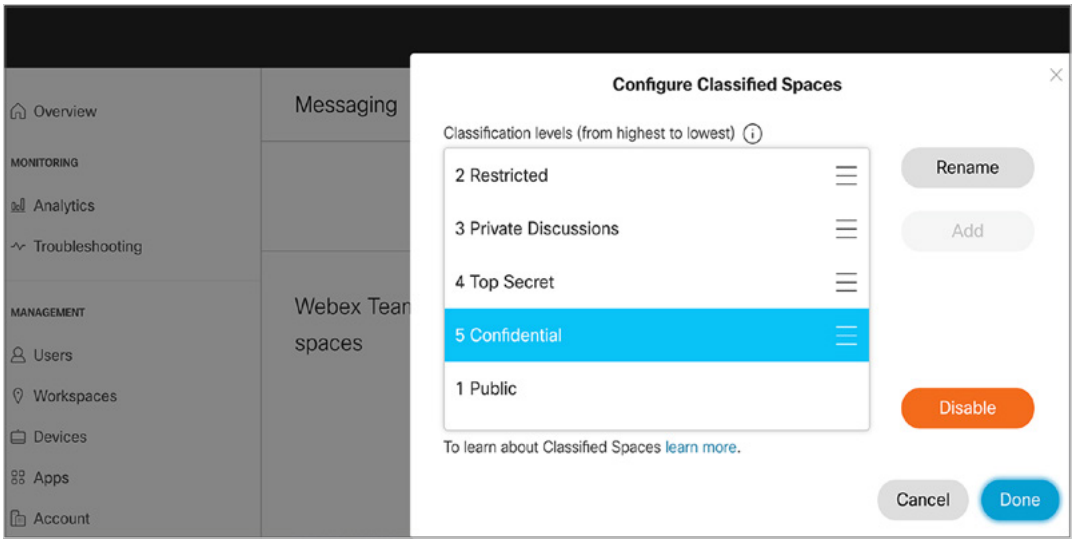

Figure 6. Control Hub configuration setting for space classification

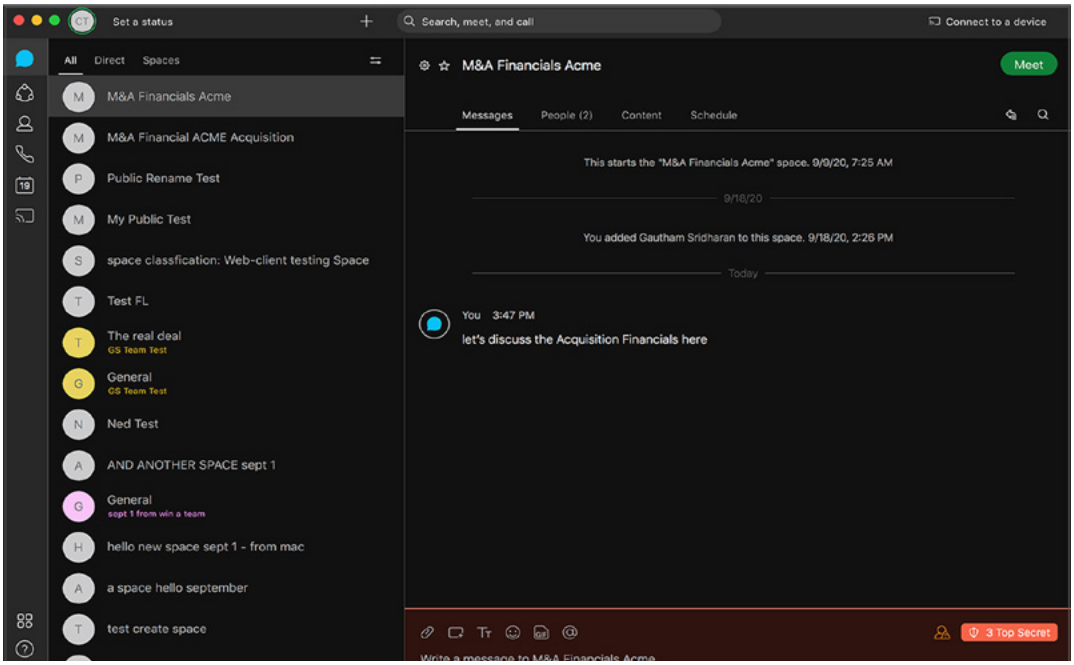

Figure 7. Control Hub space label for space classification

DLP and archival partner ecosystem

Cisco has developed key relationships with leading Cloud Access Security Brokers (CASB), DLP, and archiving vendors to protect data generated in Webex and deliver pre-integrated enterprise-grade compliance capabilities. Example of some of our industry-leading partners include:

Figure 8. Webex DLP and archival partners

Cisco on Cisco advantage and extended security options

Table 8. Available extended security options

CAPABILITIES	WEBEX
Security Bundle: Cisco Cloudlock	Integrated CASB and DLP for teams collaboration in Webex Messaging.
Security Bundle: Cisco TalosClamAV	Integrated anti-malware scan of all files uploaded and downloaded to protect users from malicious threats in Webex.

Control Hub Extended Security Pack

This Cisco on Cisco best-of-breed integrated solution can purchased and deployed very quickly to protect your company's data, your partners, and your customers. It prevents sensitive data leakage and provides anti-malware protection and multi-factor authentication.

Cisco Cloudlock for data loss prevention

- Mitigate the risk of cloud data leakage through powerful, automated response actions when sensitive data is discovered. When policies are violated, Cloudlock will automatically delete files or messages, notify users or admins, and remove users from spaces.
- Support adherence to compliance regulations within your cloud applications' security incident lifecycle directly from SIEM systems.

Cisco TalosClamAV for anti-malware protection

Cisco TalosClamAV is a built-in anti-malware engine in that scans all file uploads for Trojan attacks, viruses, malware, and other malicious threats. All files in Webex spaces that you designate will be scanned and remediated, even if they are uploaded by external users. Infected files will be marked clearly, and end users will not be able to download them on both corporate-managed and personally managed devices. Cisco TalosClamAV scans one billion files daily for over 10 million users, with 7.2 trillion attacks stopped every year.

For more information
Please visit webex.com

June 2021